Notice of Allowability	Application No.	Applicant(s)	
	10/005,105	KOCHER ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *08/07/2006*.

2. ☒ The allowed claim(s) is/are *1-19*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 8/7/06, 9/5/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail.Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Claims 1-19 have been examined.

Information Disclosure Statement

The information disclosure statements (IDSes) submitted on 08/07/2006 and 09/05/2006 were filed on the same date and after Request for Continued Examination was filed. The submission is in compliance with the provisions of 37 CFR 1.97(b)(3). Accordingly, the IDSes are being considered by the examiner.

Allowable Subject Matter

Claims 1-19 are allowed.

The following is an examiner's statement of reasons for allowance:

Claims 1 and 11, 2 and 8-10, 3-7, 12-17, and 18 and 19 are drawn to three methods for evaluating the security of a cryptographic device to recover useful information about a key, a system for evaluating the security of cryptographic hardware, and a method for analyzing externally measurable characteristics of a cryptographic device, respectively. The closest prior art, Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, and Other Systems," XP 000626590, dated 08/18/96, discloses similar methods and system. Kocher describes that, during the processing of each cryptographic operation, a plurality of measurements of an attribute related to the operation of a cryptographic device are recorded and statistically combing the recorded measurements (see § 6 Experimental Results, pages 107-109; figures 1 and 2;

measurements of modular multiplication times and modular exponentiation times). However, the above Kocher disclosure neither teaches nor suggests sending a plurality of command sequences to the device to cause the device to perform a cryptographic operation to process data using a key and determining whether information about the key is leaking from the device. These distinct steps explicitly incorporated into independent claims 1, 2, 3, 12, and 18 render claims 1 and 11, 2 and 8-10, 3-7, 12-17 and 18 and 19, respectively, allowable.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

September 19, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100